PROYECTO DE INVESTIGACIÓN

ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 EN EL ÁREA DE TI PARA LA EMPRESA MARKET MIX.

RAFAEL ANTONIO MOLANO ESPINEL

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS

BOGOTÁ D.C.

2.017

ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 EN EL ÁREA DE TI PARA LA EMPRESA MARKET MIX.

RAFAEL ANTONIO MOLANO ESPINEL

Trabajo de grado para obtener el título de
Especialista en Auditoria de Sistemas

Asesor:
NANCY EDITH OCHOA GUEVARA
PhD Tecnología Especial Educacional Florida USA

UNIVERSIDAD CATÓLICA DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
BOGOTÁ D.C.
2.017

TABLA DE CONTENIDO

Pág.

Lista de Figuras

Pág.

Lista de Gráficas

Pág.

Lista de Tablas

Pág.

Lista de Anexos

Pág.

INTRODUCCIÓN

El presente proyecto está enfocado a implementar una estrategia de un sistema de gestión de la seguridad de la información basadas en la norma ISO 27001 que permita identificar los riesgos o vulnerabilidades que amenazan la empresa Market MX obteniendo al final un diagnóstico del estado actual de la empresa Market mix, y así poder emitir las recomendaciones que deben estar acorde a la normatividad vigente.

A través de este trabajo se tomara la mejor estrategia teniendo en cuenta las normas ISO 27001 para la empresa Market Mix, empresa creada hace más de siete años y presta servicios como outsorcing y telemeracadeo a diferentes almacenes de cadena tales como: Almacenes Olímpica, Jumbo, Oxxo, Alpina, Kokoriko, Fincomercio entre otros.

Hoy en día la tecnología como hardware, software, bases de datos y redes, son herramientas estratégicas que brindan ventajas ante la necesidad de crecimiento y competitividad a los negocios, pero pueden también ocasionar pérdidas si no se administran de la mejor manera. Por eso que es necesario mantener y realizar evaluaciones periódicas de estas herramientas y del personal calificado que cumpla con el objetivo de la empresa.

Es necesario implementar una estrategia que permita establecer un Sistema de Gestión de Seguridad de la información teniendo en cuenta que la empresa Market Mix hoy en día no cuenta con los suficientes controles informáticos necesarios, es por eso que debe aplicar una estrategia de un sistema de gestión de la seguridad de la información basadas en la norma ISO 27001, que permita minimizar los riesgos a los cuales se encuentra expuesta la empresa, como perdida y daño de información, manipulación indebida de la misma entre otras.

Este trabajo permitirá a la empresa Market Mix tener una estrategia que permite ahorrar tiempo y dinero, podrá apoyarse y seguir los lineamientos que exige la norma ISO 27001 para tener un mejor control de sus actividades que pueden poner en riesgo la información de la empresa.

1. GENERALIDADES DEL TRABAJO DE GRADO

1.1 LÍNEA DE INVESTIGACIÓN

El proyecto se encuentra dentro de la línea de Software Inteligente y Covengercia tecnológica, ya que al desarrollar una estrategia para la empresa Market Mix permitirá evaluar los riesgos basados en la norma ISO 27001

1.2 PLANTEAMIENTO DEL PROBLEMA

El avance tecnológico ha permitido a las empresas implementar, herramientas y estrategias que permiten proteger la información y los sistemas, la empresa Market Mix dedicada a telemercadeo presenta algunas falencias de seguridad informática dentro de sus instalaciones que ponen en peligro las bases de datos y los sistemas de cómputo.

De manera general el Director del Equipo de Análisis e Investigación Global en América latina de la empresa Rusa de seguridad informática Karpesky lab, Dmitry Bestuzhev manifiesta lo siguiente " Colombia es uno de los países con mayor cibercriminalidad de América Latina, las grandes, medianas o pequeñas empresas son blancos de los ataques de los piratas informáticos" en encuesta realizada en abril 2013 por B2B international para Karpesky indica que en los países como Colombia, Brasil, México las medianas y pequeñas empresas pierden alrededor 45.000 dólares por cada incidente de seguridad entre los daños causados y gastos para la prevención.

No obstante debido al crecimiento exagerado de las tecnologías, no es posible tener un sistema seguro mientras tenga acceso a internet, que es una gran herramienta de búsqueda, aprendizaje, consulta e inclusive de diversión, a través de esta los sistemas o los individuos que hacen uso de ella pueden verse afectados por terceros que se encuentran al otro lado esperando la oportunidad para robar datos e información.

Es por eso que se debe tener en cuenta la implementación de herramientas, sistemas, estrategias que permitan un sitio seguro y confiable sin dejar a un lado la seguridad que debe tener el usuario de los equipos o del mismo sistema.

1.2.1 Antecedentes del problema

Actualmente la empresa Market Mix no cuenta con una estrategia que permita identificar las vulnerabilidades, riesgos que ponen en peligro la seguridad de la información y tampoco existe documentación que permita evidenciar estudios anteriores.

Es de suma importancia proteger el sistema que está compuesto por Software, Hardware, la información que se maneja e inclusive el mismo operador del sistema, la seguridad de la información tiene como principios proteger la Integridad, confidencialidad y la disponibilidad de la información.

1.2.2 Pregunta de investigación.

¿Cuál es la mejor estrategia para implementar un sistema de gestión de la seguridad de la información basada en las normas ISO 27001 en el área de TI para la empresa Market Mix?

1.2.3 Variables del problema

- **Perdida de la información**: se define como el no acceso a la información almacenada en distintos medios o sistemas de información, se puede presentar por diferentes causas en donde interviene el factor humano, ambiental, estructural o por causas externas.
- **Pérdidas financieras**: en seguridad de la información se puede determinar que las pérdidas financieras son producto de riesgos que se materializaron y no se controlaron a tiempo.
- **Pérdida de Credibilidad con los clientes:** en muchas ocasiones las empresas, entidades se ven afectadas por la pérdida de credibilidad ya que sus clientes sienten que sus datos, sus finanzas no se encuentran en lugares seguros por inconvenientes presentados en tiempos pasados o en hechos que ocurren a diario.
- **Sanciones de ley:** estas sanciones son impuestas por autoridades que observan ciertas irregularidades, o que se están violando leyes o normas interpuestas por organismos de control.

1.3 JUSTIFICACIÓN

Conforme a lo expuesto en el planteamiento del problema, es de vital importancia desarrollar una estrategia e implementar un sistema de gestión de la seguridad de la información basadas en la norma ISO 27001, para que determine o indique un diagnóstico del estado actual de la empresa Market Mix, y así lograr los ajustes necesarios teniendo en cuenta las normas establecidas.

Teniendo en cuenta que en la actualidad las empresas utilizan las plataformas tecnológicas para la prestación de servicios o la comercialización de sus productos, se hace necesario la detección temprana de las vulnerabilidades que pueden afectar el normal desarrollo de las operaciones empresariales.

Con el creciente uso del internet y la variedad de herramientas informáticas disponibles que facilitan el acceso fraudulento a las empresas, se presenta un aumento en la brecha de los controles que permiten un incremento de las amenazas a los sistemas de información, Repositorio Institucional Pontificia Universidad javeriana Vasquez Katy 2015.

En las instalaciones de la empresa no se tiene suficiente control, que cumpla con las específicas establecidas en las normas ISO 27001, exponiendo al peligro la información que se encuentra alojada en los servidores y en los sistemas de cómputo de la empresa, en ese sentido se diseñara una guía de auditoria, para la empresa MARKET MIX.

Los resultados que se obtengan del desarrollo y aplicación de la mejor estrategia, permitirá mejorar el estado actual de la empresa Market Mix , mejorando sus controles e implementándolos para nuevos proyectos o instalaciones nuevas del negocio.

1.4 OBJETIVOS

1.4.1 Objetivo general

Identificar la mejor estrategia en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información basadas en la norma ISO 27001 en el área de TI para la empresa Market Mix.

1.4.2 Objetivos específicos

- Diagnosticar a través de una matriz de estrategias el estado actual de la seguridad de la información en el área TI de la empresa Market Mix
- Aplicar los instrumentos de evaluación (Encuesta, Entrevista) al área de TI en una muestra seleccionada previamente para conocer el concepto o formas del manejo de la seguridad de la información de la empresa.
- Identificar una metodología apropiado para la aplicación de la ISO 27001 acorde a la evaluación previa en el área de TI con el fin de conocer las posibles estrategias a seguir para la seguridad de la información.
- Comprobar si la estrategia seleccionada constituyen un esquema relevante para la protección de la información en el área de TI de la empresa Market Mix.

1.4.3 Cronograma

Tabla 1. Cronograma

		FEBRERO				MARZO				ABRIL				MAYO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**ANTEPROYECTO**																																
	SELECCIÓN DEL TEMA																																
	REDACCION DEL ANTEPROYECTO																																
2	**DESARROLLO EPISTEMOLOGICO**																																
	TITULO																																
	PREGUNTA DE INVESTIGACION																																
	OBJETIVOS																																
	ESTADO DEL ARTE																																
	MARCOS																																
3	**METODOLOGIA**																																
	Enfoque y estudio dde investigacion																																
	Naturaleza, poblacion y muestra de la investigacion																																
	Recoleccion de Datos y aplicación de herramientas																																
	Analisis y tabulacion de datos																																
	esquema de las mejores estrategias para la seguridad de la informacion																																
4	**RESULTADOS Y DISCUSION**																																
	resusltados de la aplicación de la metodologia de investigacion																																
	presentacion de los resusltados por objetivos resaltando la posicion de otros autores.																																
5	**CONCLUSIONES Y RECOEMNDACIONES**																																
	conclusiones Y RECOEMNDACIONES																																
	entrega documento y sus resultados																																
	Sustentacion del proyecto de grado																																

Fuente: El autor

1.4.4 Presupuesto

Tabla 2. Presupuesto

INSUMOS	JUSTIFICACIÓN	CANTIDAD	VALOR UNITARIO	VALOR TOTAL
Resma de papel	Para la realización de las encuestas entrevistas, y los entregables.	**1**	**$ 17.000**	**$ 17.000**
Salidas trabajo de campo	Transportes para la aplicación encuestas, entrevistas 2 pasajes por cada actividad 1	**10**	**$2000**	**$ 20.000**
Tutorías	Transporte para las tutorías desde el inicio del proyecto de grado hasta la entrega final son en total 28 semanas, 2 pasajes por cada semana	**56**	**$ 2000**	**$ 112.000**
Material Bibliográfico y fotocopias	Papelería empleada en al aplicación de encuestas, entrevistas, copias de documentos e impresiones del anteproyecto y proyecto final.	**100**	**$ 100**	**$10.000**
Equipos de software y servicios técnicos	Utilización de herramientas de trabajo como equipos de cómputo, impresoras y el mantenimiento de los mismos e implementos de oficina.	**1**	**$ 100.000**	**$ 100.000**
Otros Gastos	Utilización de medios de comunicación, Plan de datos móviles y minutos	**1**	**$ 60.000**	**$ 60.000**
TOTAL				**$ 319.000**

Fuente: El autor

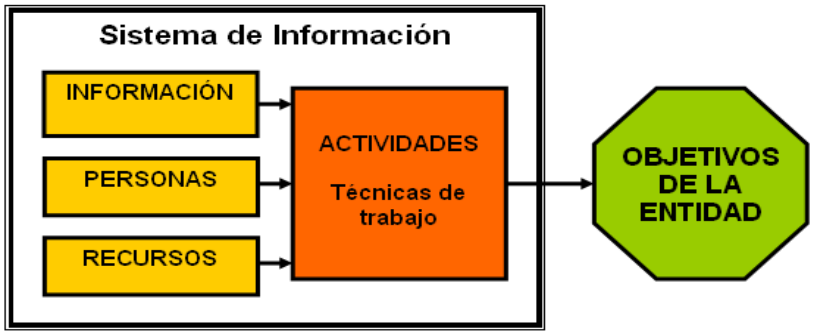
2. MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso, posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías:

- Personas
- Actividades o técnicas de trabajo.
- Datos.

Figura 1. Sistema de Información



Fuente: Disponible en: https://es.wikipedia.org/wiki/Sistema_de_información

Auditor de sistemas: persona enfocado a evaluar los sistemas de la información con el propósito de asegurar la integridad y confidencialidad y contabilidad de la información mediante las recomendaciones de seguridad y controles.

Estrategias: Conjunto de acciones que se utilizan para planificar, ejecutar con el fin de cumplir metas establecidas a un individuo o a una empresa.

Normas: Son reglas, leyes o parámetros creadas para dirigir, conservar y fomentar el orden en acciones dentro de la comunidad o una empresa.

SGSI: Sistema de Gestión de la Seguridad de la Información, son elementos utilizados

para la administración de la seguridad de la información.

Cuantitativo: hace referencia a una cantidad, valor que hace parte de un individuo u objeto, que se puede contar, medir o cuantificar.

Cualitativo: hace referencia a las cualidades que tiene una persona u objeto y se relacionan entre sí.

2.2 MARCO TEÓRICO

La palabra auditoria proviene del latin "Audire" que significa persona que tiene la virtud de oír, la auditoria se aplica en diferentes áreas y esta permite evaluar actividades, procesos, eventos y riesgos en cada uno de los objetivos específicos de áreas o de la misma empresa en general.

Actualmente a nivel mundial se utilizan procesos, modelos, métodos los cuales generan un control sobre los procedimientos de dichas organizaciones, para ello se hacen uso de políticas y normas que guían la labor del auditor. La auditoría es el resultado de un análisis o examen realizado a un grupo de procesos, áreas o personas con un fin en específico.

Hoy en día existen diferentes normas que se deben cumplir en el ámbito organizacional de las empresas, las normas ISO son estándares de seguridad establecidas por la Organización Internacional para la Estandarización y la Comisión Electrónica Internacional, ISO 27001 en ellas encontramos las mejores prácticas recomendadas en seguridad de la Información y mantener especificaciones para los Sistemas de Gestión de la seguridad de la Información (SGSI para aplicar en grandes, medianas o pequeñas empresas.

2.3 MARCO JURÍDICO

Toda organización debe tener una estrategia para la protección de su información teniendo en cuenta los estándares internacionales e implementar un Sistema de gestión de Seguridad de la Información (SGSI) siguiendo los parámetros establecidos en las normas ISO 27001, Octubre de 2005.

Ley 87 Diario oficial 41120 de la Republica de Colombia**,** Noviembre 1993 por la cual se establecen normas para el ejercicio del control interno de las entidades y los organismos del estado.

LEY ESTATUTARIA 1266 Diario oficial Nº 47.219 de la Republica de Colombia, 31 de diciembre de 2008 Contiene disposiciones legales del Habeas Data y la regulación de la protección de datos personales**.**

LEY 1273 Diario oficial 47.223 de la Republica de Colombia, Enero de 2009 modificación del código Penal, se crea un bien jurídico denominado "Protección de la información y de los datos.

LEY 1341 Diario oficial 47.426 de la Republica de Colombia, Julio de 2009, se definen los conceptos de la información y la comunicación TIC, por medio de esta ley se crea la Agencia Nacional del Espectro.

Ley estatutaria 1581, Diario oficial 48.587 de la Republica de Colombia, Octubre de 2012 por la cual se dictan disposiciones generales para la protección de datos personales, siguiendo la sentencia C-748 de 2011 de la Corte Constitucional y el Congreso de la Republica.

2.3.1 Estándares

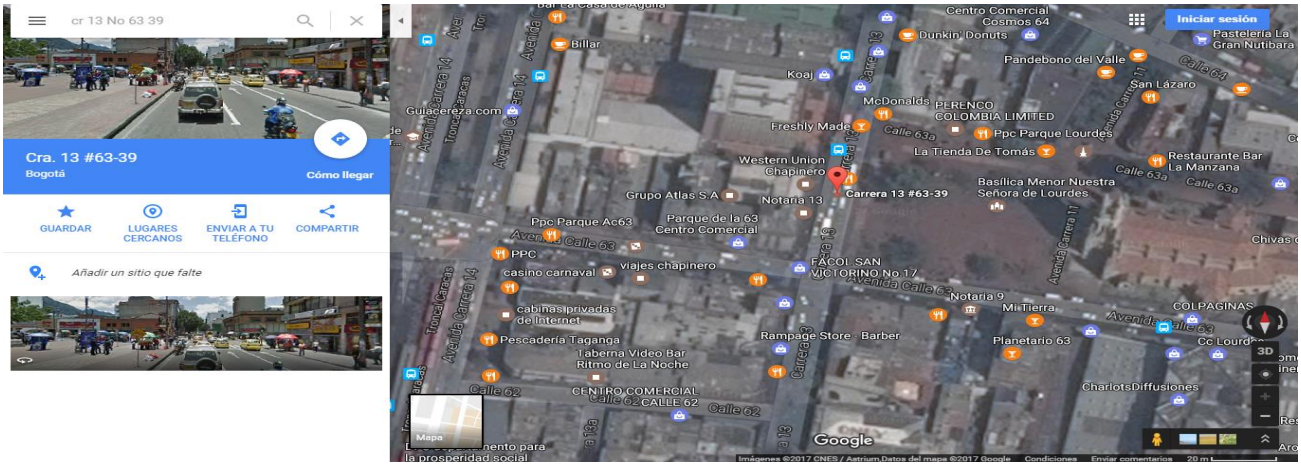
ISO/IEC 27001 aprobado y publicado por International Organization for standardization e International Electrotechnical **,** 2005 contiene los parámetros que contiene parámetros para la seguridad de la información.

ISO 27002 aprobado y publicado por International Organization for standardization e International Electrotechnical 2007 contiene las recomendaciones de las mejores practicas para la seguridad de la Información.

2.4 MARCO GEOGRÁFICO

La empresa objeto del proyecto se encuentra ubicada en la Carrera 13 Nº 63 -39 interior 7 en la localidad de Chapinero de la ciudad de Bogotá D.C.

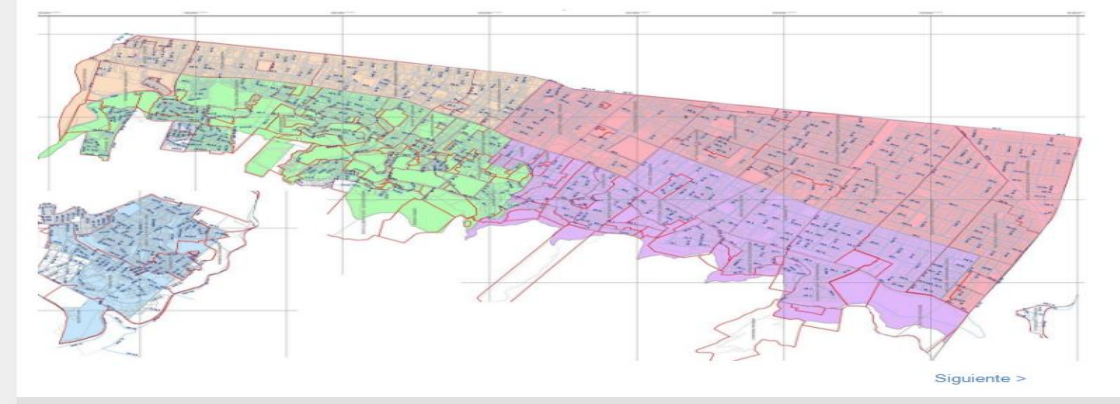
Figura 2. Ubicación Empresa



Fuente: Google Maps

La localidad de Chapinero se encuentra al nororiente de la ciudad de Bogotá y se divide en tres sectores: Chapinero (barrio), el Lago y Chicó; actualmente cuenta con 131.027 habitantes, y sus área es de 3.899 hectáreas, dividida en cinco (5) Unidades de Planeación Zonal (UPZ) y una Unidad de Planeación Rural (UPR) en total cuenta con 50 barrios.

Figura 3. Mapa localidad II de Chapinero



Fuente: Disponible en internet en: http://www.chapinero.gov.co/

En Chapinero hay tres sectores de gran importancia comercial en la figura numero 3 observamos el mapa de la localidad y de ella podemos que se encuentra dividida en los

siguientes sectores:

- Zona Rosa, alrededor de la Calle 82, entre las Carreras 11 y 15, se encuentran galerías de arte, almacenes y tiendas que venden artículos para regalo y uso personal. “La Calle del Sol”, Carrera 14 entre Calles 82 y 84, agrupa excelentes y exclusivas boutiques, diseñadores y casas de alta costura. En las Calles 79 B y 80 entre Carrera Séptima y Avenida Novena se encuentra gran cantidad de anticuarios.
- Gran Chapinero, se extiende a lo largo de la Avenida Caracas y de la Carrera 13, el comercio se extiende básicamente sobre este eje, cuyo núcleo es la Plaza de Lourdes. Posee almacenes de ropa, artículos de cuero y calzado, telas, adornos, librerías, papelerías y disco tiendas. Cuenta con algunos centros comerciales, en este sector especìfico de la localidad se ubica la empresa Market Mix.
- Avenida 100, donde se ha instalado la hotelería que atrae de preferencia a los ejecutivos de empresas, con buena dotación de ayudas comerciales, comunicaciones, informática, etc. y muchos sitios de encuentro para hombres de negocios, es el sector de mayor costo. Es el límite que divide Chapinero y Usaquén. Allí se encuentra el World Trade Center de Bogotá y su importancia como zona de negocios es única en la ciudad.
- A nivel comercial es el sector más próspero de Bogotá, ya que cuenta con establecimientos dignos de grandes capitales mundiales cómo el Hard Rock Café ubicado en el C.C. Atlantis Plaza, las tiendas de Versace, Swarovski, MNG, Mac Center, Tower Records, y otras ubicadas en el C.C. El Retiro, y la tienda Louis Vuitton en el centro comercial Andino que en su gran mayoría son las tiendas más exclusivas.

2.5 MARCO DEMOGRÁFICO

La empresa Market Mix cuenta con un total 200 empleados entre hombres y mujeres que se encuentran en un rango de edad entre los 21 a 40 años, resientes en las diferentes localidades de la ciudad de Bogotá D,C y cuentan con perfiles de técnicos, tecnólogos , profesionales y practicantes del SENA, esta información se puede constatar en las planillas de pago de nómina y seguridad social de la empresa.

En el área de TI cuenta con 20 trabajadores, que desempeñan diferentes cargos como desarrollo de aplicaciones, soporte o help desk, atención al usuario, mantenimiento de equipos y operarios de los diferentes equipos de cómputo.

2.6 ESTADO DEL ARTE

El impacto que fomentan las TIC en la vida cotidiana han permitido que se realicen investigaciones más a fondo para así poder aplicarlas dentro y fuera de nuestros hogares o lugares de trabajo, hago referencia de algunos artículos, ensayos y tesis que tratan de la norma que se pretende tener en cuenta para mejorar la seguridad de la información en la empresa Market Mix.

En el Articulo de divulgación del señor Arean Hernando Velazco Melo, Abogado y Magister en informática en junio de 2008, pretende informar sobre la existencia de diversas modalidades que incluye el derecho informático y crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información, se utiliza como metodología de investigación la norma ISO 27001 que hace referencia y comprende la protección de datos personales, la contratación de bienes informáticos y telemáticos.

"Tesis Diseño de un sistema de gestión de seguridad de la información para cooperativas de ahorro y crédito en base a las normas ISO 27001", Mantilla 2009, se muestra como identificar evaluar y gestionar el riesgo.

"Examen complexivo, propuesta para la implementación de controles de seguridad basado en ISO 27001" Arce 2016, en este ensayo se presenta el estado actual del proceso de implementación de las ISO 27001 en los laboratorios del colegio Atahualpa de la ciudad de Machala.

"Tesis Análisis De Vulnerabilidades A Nivel De Acceso Lógico Basado En La Norma ISO/IEC 27001 En La Comunidad Provincia De Nuestra Señora De Gracia De Colombia" Castro 2010

"Tesis Protección Contra Código Malicioso Y Gestión De Seguridad De Las Redes Basado En La Norma ISO/IEC 27001 en La Empresa Provincia De Nuestra Señora De Gracia

De Colombia" Collazos 2010.

"Tesis diseño e Implementación de un Sistema de Gestión de Seguridad de información en Procesos Tecnológicos" Barrantes, Herrera 2012

3. METODOLOGÍA

3.1 ENFOQUE DE LA METODOLOGÍA

El enfoque de esta investigación es de carácter mixto cualitativo, cuantitativo toda vez que lo que se pretende es realizar una recolección de datos, mediante encuesta cerrada y entrevista abierta, basadas en la observación, análisis y evaluación cuantitativa, elaboradas por el área de auditoría de procesos relacionada a la metodología de desarrollo de aplicaciones y controles de cambio de sistemas en la empresa Market Mix.

3.2 TIPO DE ESTUDIO

Esta investigación es de carácter descriptivo ya que permite la observación e interpretación de resultados obtenidos en la recolección de información mediante las encuestas y entrevistas realizadas, Méndez (2003) manifiesta "la investigación descriptiva utiliza criterios sistemáticos que permiten poner de manifiesto la estructura de los fenómenos en estudio, además ayudan a establecer comportamientos concretos mediante el manejo de técnicas específicas de recolección de información".

3.3 UNIVERSO DE LA INVESTIGACIÓN

3.4 POBLACIÓN

La investigación se desarrolla tomando como referencia el equipo de trabajadores de la empresa Market Mix, el cual está compuesto por un grupo multidisciplinario de 200 empleados que se encuentran distribuidos en las diferentes áreas administrativas y operativas.

3.5 MUESTRA

Después de haber definido el área de la empresa, se toma la muestra que corresponde a un

total de 20 personas encuestadas del área de TI, teniendo en cuenta que en esta área se desarrollan los procesos que se encuentran sujetos a la investigación, se debe tener en cuenta que no se revelaran datos del personal encuestado ya que es una información privada de la empresa haciendo uso a la ley de protección de datos.

Tabla 3. Cumplimiento de Categorías

Categorías	Indicadores	Cumplimiento Numero de Objetivos
Conocimiento en Seguridad de la información	Evaluar el grado de conocimiento de los usuarios Capacitación del personal del área de TI Evaluar la capacitación realizada al personal de TI	1, 2 ,3,4
Técnicas para la protección de datos y seguridad de la información	Verificar la realización de los backup Verificación proveedores alternos Verificación servidor alterno Identificar la metodología apropiada para la aplicación de las normas ISO	1,2,3,4
Aplicación de herramientas para la protección de datos y seguridad de la información	Herramientas de protección de datos y seguridad de la información.	2,4

Fuente: El autor

3.6 INSTRUMENTOS DE EVALUACIÓN

3.6.1 Encuesta

Para obtener la información se seleccionaron 20 preguntas donde se involucran personas, procesos y equipos, que servirán para tomar las muestras necesarias y realizar su análisis mediante el método de Likert, el formato está dividido en tres categorías y se evalúan mediante la siguiente escala de valoración, Excelente (5), Bueno (4) No tiene Conocimiento (3), Muy Deficiente (3) y Regular (1), su alcance tiene como objetivo evaluar los conocimientos de las personas encuestadas, el estado de los equipos y los procesos realizados en el área de TI.

3.6.2 Entrevista

La entrevista fue realizada a 5 profesionales del área de TI tomando como referencia 5

preguntas del cuestionario realizado en las encuestas, donde se busca conocer los conceptos que tienen con respecto a la seguridad de la información.

3.7 FASES DEL TRABAJO

El desarrollo de este trabajo fue hecho a través de las siguientes fases.

Tabla 4. DOFA

DEBILIDADES	FORTALEZAS
No se tiene un amplio conocimiento sobre la seguridad de la información	La empresa cuanta con servidor alterno para guardar los backup`s realizados en caso de algún evento.
Las Normas de seguridad son poco conocidas para el personal del área de TI	Se cuenta con proveedor de servicios alterno que facilita la continuidad del negocio en caso de algún inconveniente que presente el otro.
Los Backus no son revisados después de realizados	El licenciamiento de la empresa Market Mix es legal
El acceso al área de servidores no se encuentra bien protegida.	Cuenta con el área de soporte técnico dentro de la empresa y no depende de terceros.
El antivirus utilizado no brinda una seguridad completa	Los password protegen el ingreso de usuarios no autorizados para el uso de los equipos de la compañía.
Los backup`s se revisan de forma inadecuada (por peso)	El área de TI tiene personal calificado
Falta capacitación con respecto a seguridad de la información.	
OPORTUNIDADES	**AMENAZAS**
Contar con el presupuesto para la compra e innovación de las herramientas para tener una mejor seguridad de la información.	Perdida de información por no revisar las copias de seguridad después de que se ejecuten
Adquirir nuevas tecnologías para la seguridad de la información	Pérdidas financieras debido a las sanciones impuestas por la ley.
Realizar capacitaciones constantemente al personal	Afectación de las bases de datos por el ingreso a paginas no permitidas

Fuente: El autor

3.7.1 Fase I

Se realiza análisis de la matriz DOFA para analizar las Debilidades, Oportunidades, Fortalezas y las Amenazas que se están presentando en el área de TI de la empresa Market Mix

de acuerdo a la información recolectada en el trabajo de campo.

3.7.2 Fase II

Se realiza la aplicación de los instrumentos mencionados (Encuesta, Entrevista) a la población de muestra, que es objeto de estudio en el área de TI de la empresa Market Mix, la encuesta fue procesada por escala de Likert y la entrevista se obtienen los conceptos emitidos por los líderes o integrantes del área de TI con más nivel jerárquico a través de un mapa conceptual, esta información permitirá medir el nivel de conocimientos con respecto a los tres ítem de evaluación que se registraron en la encuesta.

3.7.3 Fase III

Se tuvieron en cuenta tres metodologías, para realizar la identificación de la herramienta que se ajuste a lo establecido dentro del trabajo de grado y las normas que se tendrán en cuenta para el desarrollo de la estrategia para la empresa Market Mix.

Se analizaron las siguientes metodologías: (NIST SP 800, OCTAVE, PHVA) encontrando las siguientes desventajas, **NIST SP 800:** En su modelo no tiene contemplados los procesos, los activos y las dependencias, **OCTAVE:** No tiene en cuenta el principio de no repudio de la Información, utiliza muchos documentos, se requieren amplios conocimientos técnicos, se debe comprar licencia, se selecciona la metodología PHVA (Planear, hacer, verificar, Actuar), ya que brinda las mejores opciones para implementar el SGSI en el área de TI de la empresa Market Mix, la metodología se ajusta a lo exigido en el estándar ISO 27001,y de acuerdo a lo investigado es la metodología más usada para la implementación de los Sistemas de Gestión de seguridad de la Información, cabe resaltar que la metodología es muy completa y su desarrollo es de fácil adecuación para las empresas.

La metodología PHVA o ciclo de Deming está basada en un concepto ideado por Walter Shewhart, esta metodología es muy utilizada en los Sistemas de Gestión de seguridad de la Información SGSI y los Sistemas de Gestión de la calidad SGC, se divide en cuatro pasos que se definen de la siguiente manera:

Planear: Establecer los objetivos y procesos necesarios para conseguir los resultados, en

este paso podemos tener en cuenta lo siguiente, el que, como y para que se planeó.

Hacer: Implementar los procesos, se debe tener en cuenta los datos recolectados, quien los recolecto, cuando y como se realizó.

Verificar: Realizar seguimiento y la medición a productos y procesos, se debe tener en cuenta si lo realizado fue lo que se planeó, si se lograron los resultados, y que análisis se realizó a los resultados.

Actuar: Tomar acciones para mejorar continuamente el desempeño de los procesos, en este último paso debemos indagar sobre que aprendizaje hubo, que cambios se adoptaron y que acciones correctivas se realizaron.

3.7.4 Fase IV

Se realizara la evaluación de la guía por expertos en seguridad informática.

4. RESULTADOS

Se realiza trabajo de campo diligenciando un formato tipo encuesta cerrada al líder del área de TI de la empresa Market Mix, y de acuerdo a la información recolectada se procede a realizar la matriz DOFA, con los resultados obtenidos de la matriz se evidencian las debilidades y amenazas que pueden afectar la seguridad de la información, es por eso que se hace necesario aplicar las entrevistas y encuestas al personal del área de TI, bajo tres ítems de evaluación (Conocimientos de Seguridad Informática, Técnicas para la Protección de Datos y Aplicación de Herramientas para la Protección de Datos y Seguridad de la Información)

Después de haber aplicado, analizado y procesado las encuestas y entrevistas por la escala de Likert, se obtuvo como resultado las siguientes gráficas y valores que permiten ver el estado actual del área de TI con respecto a los tres ítems evaluados.

4.1 CONOCIMIENTO EN SEGURIDAD DE LA INFORMACIÓN

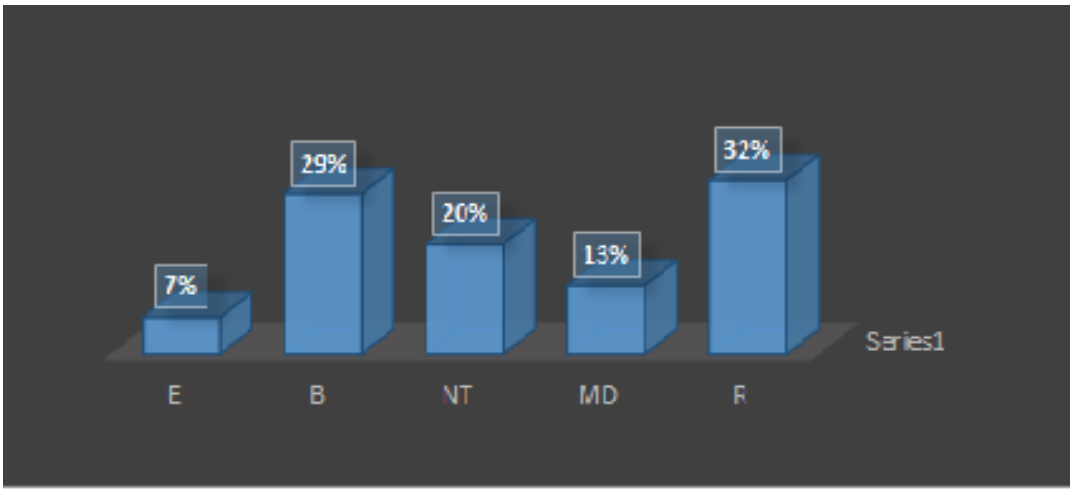
De las 20 encuestas realizadas al personal en el área de TI, se logra evidenciar que el 7% su conocimiento es excelente, el 29 % su conocimiento es bueno, el 20% no tiene conocimiento, el 13% su conocimiento es muy deficiente y el 32% su conocimiento es regular, se puede definir que la mayoría del personal esto es 65% que labora en el área de TI tiene unos niveles de conocimiento de seguridad de la información muy bajos, o no los tiene, es de suma importancia establecer tareas o actividades que conlleven a que el personal nivele los conocimientos de seguridad informática .

Tabla 5. Conocimientos en la Seguridad de la seguridad de la información

1 Conocimiento en la Seguridad de la informacion	E	B	NT	MD	R
Que conocimientos posee con respecto a la seguridad de la información	2	8	1	6	3
Que conocimientos tiene sobre las normas que establecen de Seguridad de la información.	2	5	6	0	7
Qué nivel de conocimiento adquiere a través de las capacitaciones realizadas en seguridad de la información por parte de la empresa.	2	12	1	0	5
El contenido de las evaluaciones es adecuado para medir los conocimientos adquiridos en las capacitaciones con respecto a seguridad de la información.	0	6	0	0	14
Cual es su conocimiento sobre Normas ISO 27001.	1	1	10	6	2
Que conocimiento tiene sobre la ley de protección de datos	1	3	6	3	7
	7%	29%	20%	13%	32%

Fuente: El autor

Gráfica 1. Porcentaje Conocimientos



Fuente: El autor

4.2 CONOCIMIENTO EN TÉCNICAS PARA LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

De las 20 encuestas realizadas al personal en el área de TI, se logra evidenciar que el 1% su conocimiento es excelente, el 11 % su conocimiento es bueno, el 38% no tiene conocimiento,

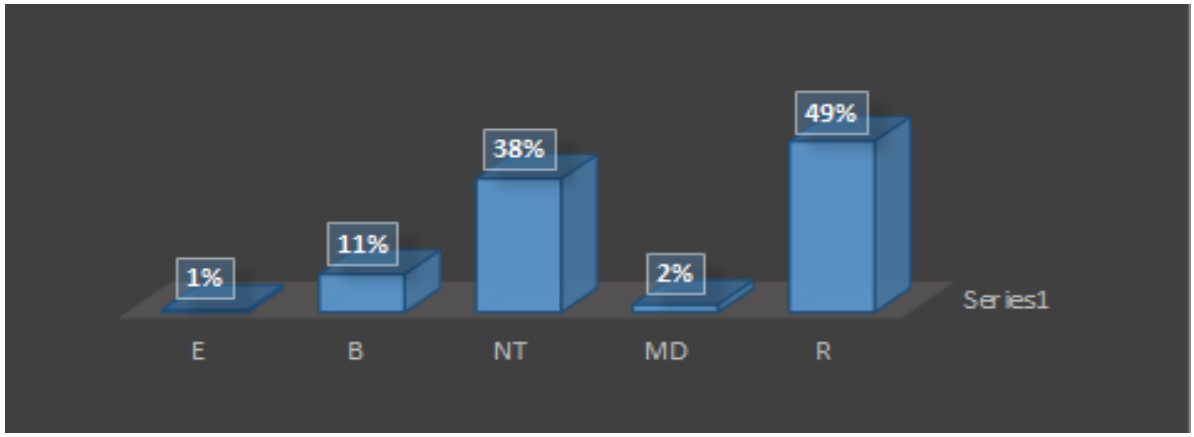
el 2% su conocimiento es muy deficiente y el 49% su conocimiento es regular, se puede definir que la mayoría del personal esto es 89 % que labora en el área de TI tiene unos niveles de conocimiento de las técnicas para la protección de datos y seguridad de la información muy bajos, o no los tiene, es necesario implementar una estrategia que permitan reducir los riesgos que pongan en peligro la disponibilidad, la integridad y confidencialidad de la información en la empresa Market Mix.

Gráfica 2. Conocimientos para la Protección de Datos y Seguridad de la Información

2. Tecnicas para la Proteccion de datos y Seguridad de la Informacion	E	B	NT	MD	R
El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?	1	4	10	0	5
Los datos que se verifican después de realizadas las copias de seguridad se catalogan como:	0	0	12	0	8
El servicio prestado por el operador alterno en caso de que el principal falle lo podemos definir como:	0	4	9	1	6
En qué estado se encuentra el servidor alterno.	0	6	11	0	3
El Sistema de control para el ingreso a esta área se define como.	0	1	3	2	14
Como se define las pistas dejadas al ingresar a esta área	0	0	4	0	16
Como se definen los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.	0	0	4	0	16
	1%	11%	38%	2%	49%

Fuente: El autor

Gráfica 3. Porcentaje del conocimiento



Fuente: El autor

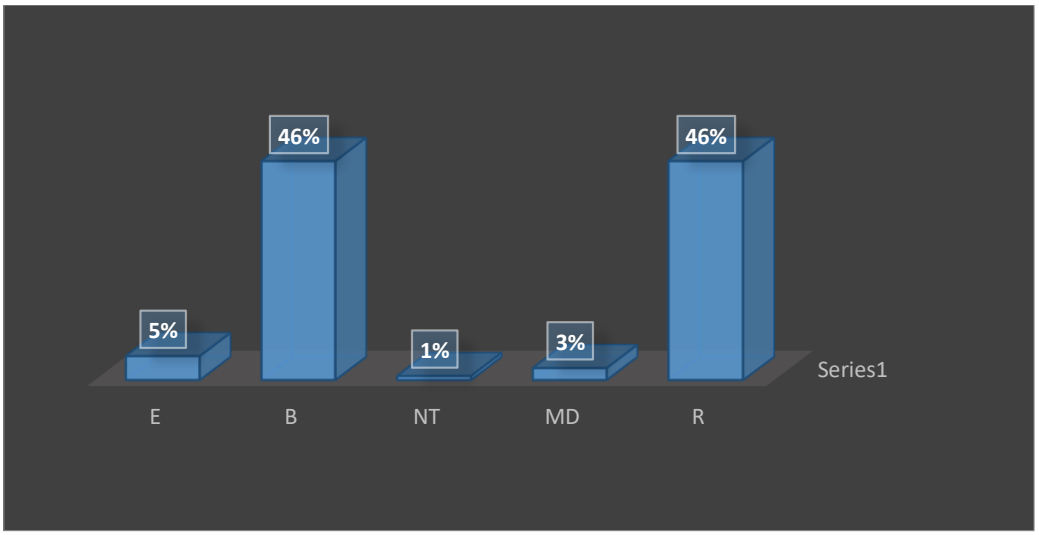
4.3 APLICACIÓN DE HERRAMIENTAS PARA LA PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN

Tabla 6. Aplicación de herramientas para la protección de Datos y Seguridad de la Información

3. Aplicación de Herramientas para la protección de datos y la Seguridad de la Información	E	B	NT	MD	R
El antivirus instalado en los equipos de cómputo de la empresa se puede definir como	1	9	0	1	9
El nivel de protección brinda el antivirus instalado en los equipos de computo	1	6	0	1	12
Como se define la restricción a paginas no permitidas en la empresa Market Mix	0	0	1	1	18
Los equipos de cómputo tienen licenciamiento vigente	4	10	0	0	6
Como se define el password para el ingreso al sistema	0	14	0	0	6
El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.	0	16	0	0	4
	5%	46%	1%	3%	46%

Fuente: El autor

Gráfica 4. Porcentaje Conocimiento



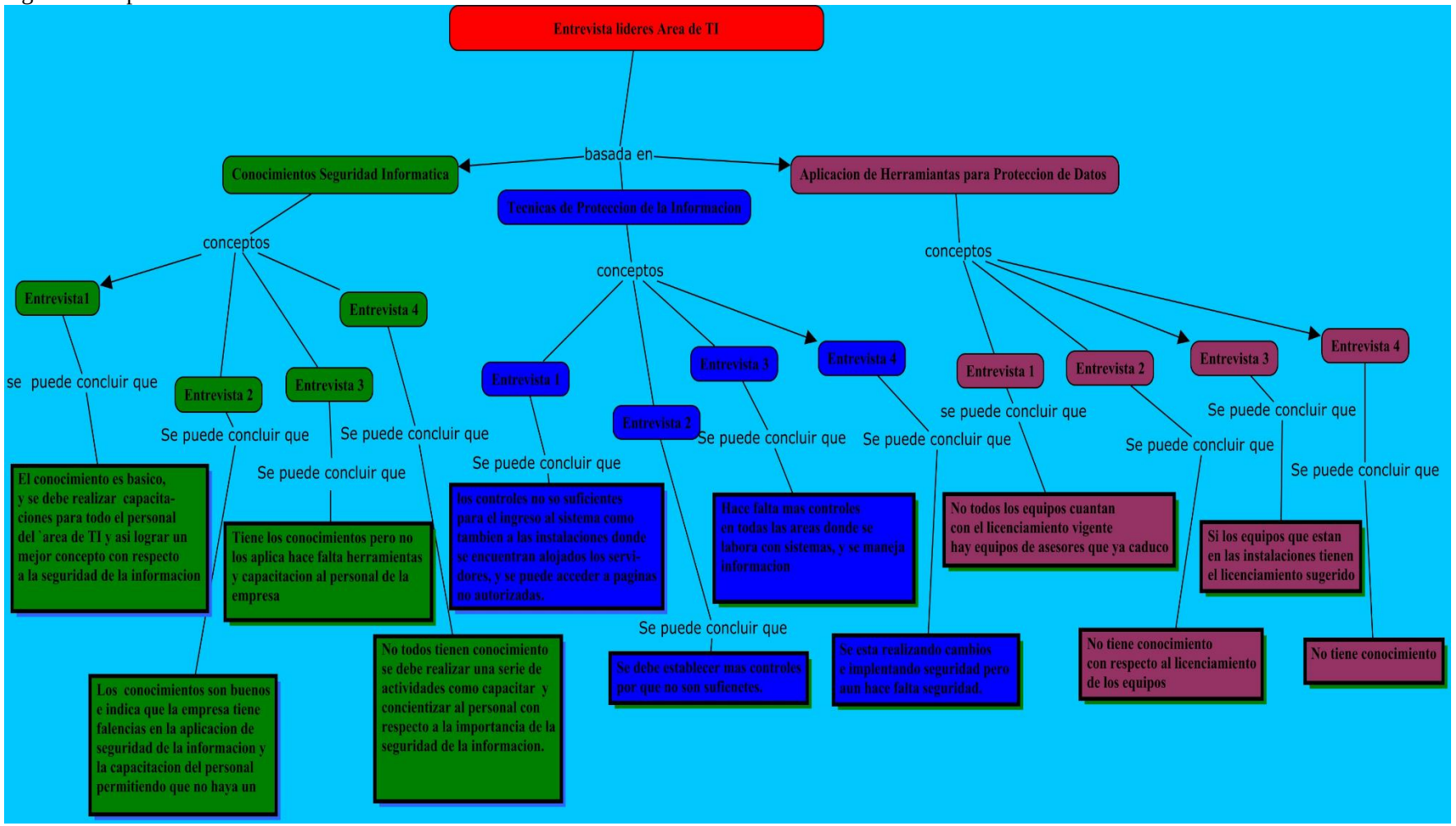
Fuente: El autor

De las 20 encuestas realizadas al personal en el área de TI, se logra evidenciar que el 5% su conocimiento es excelente, el 46 % su conocimiento es bueno, el 1% no tiene conocimiento, el 3% su conocimiento es muy deficiente y el 46% su conocimiento es regular, en este ítem se evidencia que el índice de des favorabilidad hacía los conocimientos de la aplicación de las herramientas para la protección de datos y seguridad de la información cambia de una manera favorable, pero esto no deja de ser un riesgo para la seguridad de la información ya que aún se presentan porcentajes muy altos en personal que tiene conocimientos muy regulares, y es indispensable realizar la implementación de la metodología seleccionada para cumplir con las tareas y actividades que esta señala.

4.4 RESULTADOS DE LA ENTREVISTA

Después de haber realizado la entrevista con los cuatro líderes del área de TI que ostentan el título de profesional se evidencia que tienen y poseen los conocimientos en cuanto a los tres ítem evaluados (Conocimiento en Seguridad de la Información, Técnicas para la Protección de Datos y seguridad de la información y aplicación de Herramientas para la Protección de datos y Seguridad de la Información) pero no los aplican dentro de la empresa, de esta entrevista se obtienen el siguiente mapa mental, donde se observa la información suministrada por los entrevistados, los resultados se encuentran en el anexo Nº

Figura 4. Mapa Mental Entrevista



Fuente: El autor

4.5 MÉTODO DE TRIANGULACIÓN

El método de triangulación permite validar los resultados que se obtuvieron o se recolectaron mediante la aplicación de un trabajo de campo o la aplicación de varias metodologías con el fin de tener un concepto desde diferentes puntos de vista, es por eso que empleara este método para obtener un punto más detallado de lo realizado en esta investigación.

Partiendo del método de triangulación se puede establecer que los resultados obtenidos en las encuestas que hay un porcentaje muy alto en el desconocimiento de los ítems evaluados, la información recolectada en las entrevistas, las personas que participaron de ella cuentan con los conocimientos sobre los temas pero no los aplican porque no pueden transmitirlos a todo el personal involucrado de la empresa, la matriz DOFA permitió detallar las amenazas y vulnerabilidades que se pudieron realizar a través del trabajo de campo realizado en la empresa MarKet Mix.

4.6 METODOLOGÍA PHVA

De acuerdo a los resultados obtenidos en la aplicación de las encuestas, entrevistas y matriz DOFA donde se detectaron las amenazas y vulnerabilidades que tiene el área de TI la metodología seleccionada PHVA (Planear, Hacer, Verificar y actuar) se ejecutara de la siguiente manera:

PLANEAR

- Identificar el problema.
- Realizar cronograma de actividades
- Establecer objetivos para el mejoramiento de los ítems evaluados.
- Asignar funciones a cada persona para tener un mejor control de las actividades
- Establecer reglas de cumplimiento

HACER

- Desarrollar el cronograma
- Realizar capacitaciones al personal de la empresa
- Implementar los procesos
- Fomentar el trabajo en equipo

ACTUAR

- Tomar las acciones para mejorar el desempeño de los objetivos propuestos
- Verificar sobre lo aprendido
- Indagar sobre los cambios que se realizaron si sirvieron
- Tomar correctivos
- Verificar las metas propuestas
- Tomar decisiones si hay que cambiar procedimientos.

VERIFICAR

- Realizar seguimiento a las actividades programadas
- Evaluar las capacitaciones
- Verificar que las funciones asignadas se estén cumpliendo
- Verificar si los objetivos se están cumpliendo
- Se debe validar si lo que se está realizando es lo que se planeó.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El objetivo de este trabajo de grado era identificar una estrategia para la implementación de un Sistema de Gestión de Seguridad de la Información para el área de TI de la empresa Market Mix, después de haber seleccionado las herramientas que permitieron la evaluación del estado actual del área de TI, los datos arrojados se procesaron y permitieron que se identificara la mejor estrategia que se debe desarrollar paso a paso con el fin de cumplir con los objetivos de la misma.

La aplicación de la estrategia y el monitoreo constante de las labores y responsabilidades asignadas a cada uno de los integrantes, permitirán identificar los riesgos a los que están expuestos dentro de la organización, así mismo atacarlos y realizar las correcciones pertinentes con el fin de hacer mejoras continuas y proteger la información para que no se vea afectada la empresa.

5.2 RECOMENDACIONES

Se debe crear un comité o grupo de seguridad con el fin de establecer funciones y responsabilidades para un mejor control de las actividades a realizar.

Se debe realizar capacitaciones constantes para nivelar los conocimientos del personal que labora no solo dentro del área de TI sino también para toda la empresa concientizándolos de la importancia de la seguridad de la información.

Se debe realizar pruebas constantes con el otro proveedor del servicio de internet con el fin de garantizar la continuidad del negocio en caso de que el operador principal falle.

Los Backup`s se deben verificar si todos los datos alojados en el momento de realizarlo se copiaron en su totalidad y no como se viene manejando actualmente que es por su peso.

Se debe mejorar la seguridad para el ingreso al área de los servidores ya que una bitácora no certifica que todo el personal que ingreso se haya registrado debidamente, se debe hacer

demasiado énfasis en la seguridad y en la protección de la información y los activos donde se alojan todas las bases de datos.

6. REFERENCIAS BIBLIOGRÁFICAS

Alemán Novoa, H., & Rodríguez Barrera, C. (2015). *Metodología para el análisis de riesgos en los SGSi.* Obtenido de Publicaciones e Investigacion EAN: http://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Arias Valencia, M. M. (Abril de 1999). *La triangulación metodológica: sus principios, alcances y limitaciones.* Obtenido de Udea.com: https://www.uv.mx/mie/files/2012/10/Triangulacionmetodologica.pdf

Ávila García, V. (8 de Octubre de 2010). *La triangulación, una técnica de investigación.* Obtenido de Triangulación: http://triangulacion-tecnicadeinvest.blogspot.com.co/

C.M., J. (23 de Marzo de 2014). *Metodologías de Evaluación en Riesgos Informáticos.* Obtenido de http://metodosdeevaluacionderiesgos.blogspot.com.co/2014/03/metodologias-de-evaluacion-de-riesgos.html

Club de la Securite de L´Information Francais. (2010). *Mehari.* Obtenido de www.mehari.info: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf

SGSI. (5 de Mayo de 2016). *¿Cómo utilizar la serie SP 800 de la norma ISO 27001?* Obtenido de Blog Especializado en Sistemas de Gestión de Seguridad de la Información: http://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/

ANEXOS

Anexo A. Encuesta cerrada

ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 EN EL ÁREA DE TI PARA LA EMPRESA MARKET MIX

UNIVERSIDAD CATOLICA DE COLOMBIA
ENCUESTA CERRADA

Objetivo: Determinar el nivel de seguridad de la información en el área de TI Basada en las normas ISO 27001 en la empresa Market Mix, para seleccionar la mejor estrategia a seguir.

Proceso de confiabilidad: se protege los datos personales de los encuestados siguiendo los parámetros establecidos en la ley estatutaria 1581 del 17 de Octubre de 2012.

Datos Demográficos
Cargo_____ Antigüedad en la empresa Nivel de educación : Técnico ☐ Tecnólogo ☐ Profesional ☐ Otros ☐

Marque con una x en las casillas correspondiente la opción que considere pertinente

[E]xcelente (5) **[B] Bueno** (4) **[NT] No tiene Conocimiento** (3)

[MD] Muy deficiente (2) **[NT]** regular (1)

Datos cumplimiento de los indicadores						
Categorias / Indicadores		**E (5)**	**B (4)**	**NT (3)**	**MD (2)**	**R (1)**
1. Conocimiento en Seguridad de la información						
1.1 La empresa Market Mix a impartido la capacitación adecuada en cuanto normas de seguridad de la información teniendo en cuenta lo siguiente:						
1.2	Que conocimientos posee con respecto a la seguridad de la información					
1.3.	Que conocimientos tiene sobre las normas que establecen de Seguridad de la información.					
1.4	Qué nivel de conocimiento adquiere a través de las capacitaciones realizadas en seguridad de la información por parte de la empresa.					
1.5	El contenido de las evaluaciones es adecuado para medir los conocimientos adquiridos en las capacitaciones con respecto a seguridad de la información.					
1.2 Conocimiento de la normatividad						
1.6	Cual es su conocimiento sobre Normas ISO 27001.					
1.7	Que conocimiento tiene sobre la ley de protección de datos					
2. Tecnicas para la protección de datos y seguridad de la informacion						
2.1 Para la protección de la información se debe tener en cuenta lo siguiente						

2.2.	El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?					
2.3.	Los datos que se verifican después de realizadas las copias de seguridad se catalogan como:					
2.4.	El servicio prestado por el operador alterno en caso de que el principal falle lo podemos definir como:					
2.5.	En qué estado se encuentra el servidor alterno.					
2.2 Acceso a el área de servidores o Backup						
2.6.	El Sistema de control para el ingreso a esta área se define como.					
2.7.	Como se define las pistas dejadas al ingresar a esta área					
2.8	Como se definen los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.					
3. Aplicación de herramientas para la protección de datos y seguridad de la informacion						
3.1 Herramientas para la protección de datos y seguridad de la información						
3.2	El antivirus instalado en los equipos de cómputo de la empresa se puede definir como					
3.3	El nivel de protección brinda el antivirus instalado en los equipos de computo					
3.4	Como se define la restricción a paginas no permitidas en la empresa Market Mix					
3.5	Los equipos de cómputo tienen licenciamiento vigente					
3.2 Estrategia para la protección de la información						
3.6	Como se define el password para el ingreso al sistema					
3.7	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.					

Anexo B. Entrevista abierta

ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 EN EL ÁREA DE TI PARA LA EMPRESA MARKET MIX

UNIVERSIDAD CATÓLICA DE COLOMBIA
ENTREVISTA ABIERTA PARA LÍDERES

Objetivo: Determinar el nivel de seguridad de la información en el área de TI Basada en las normas ISO 27001 en la empresa Market Mix, para seleccionar la mejor estrategia a seguir.

Proceso de confiabilidad: se protege los datos personales de los encuestados siguiendo los parámetros establecidos en la ley estatutaria 1581 del 17 de Octubre de 2012.

Datos Demográficos
Cargo_____ Antigüedad en la empresa Nivel de educación : Técnico ☐ Tecnólogo ☐ Profesional ☐ Otros ☐ Cual:

	Categorias / Indicadores		**OBSERVACIONES**
1	Que conocimientos posee con respecto a la seguridad de la información		
2.	Que conocimientos tiene sobre las normas que establecen la Seguridad de la información.		

3	Cuál es su conocimiento sobre Normas ISO 27001.		
4	Que conocimiento tiene sobre la ley de protección de datos		
5	Los equipos de cómputo tienen licenciamiento vigente		
6	El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.		

Anexo C. Escala de Likert

ENCUESTADO / ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Total
1. Conocimiento en la Seguridad de la Informacion																					
Que conocimientos posee con respecto a la seguridad de la información	2	1	4	2	3	4	2	4	5	4	5	4	4	4	1	4	2	2	1	2	20
Que conocimientos tiene sobre las normas que establecen de Seguridad de la información.	1	1	1	1	3	4	3	4	5	4	5	3	4	1	1	4	3	3	1	3	20
Qué nivel de conocimiento adquiere a través de las capacitaciones realizadas en seguridad de la información por parte de la empresa.	4	4	4	4	4	4	4	5	4	4	5	4	4	1	4	1	1	1	1	3	20
El contenido de las evaluaciones es adecuado para medir los conocimientos adquiridos en las capacitaciones con respecto a seguridad de la información.	1	4	1	1	1	1	1	1	4	4	4	4	4	1	1	1	1	1	1	1	20
Cual es su conocimiento sobre Normas ISO 27001.	3	3	2	2	3	2	2	3	1	1	5	3	2	3	2	4	3	3	3	3	20
Que conocimiento tiene sobre la ley de protección de datos	1	1	2	2	3	1	1	2	4	4	5	1	1	3	1	4	3	3	3	3	20
2. Tecnicas para la Proteccion de Datos y seguridad de la informacion																					
El medio donde se alojan los backup de los servidores en ¿qué estado se encuentra?	3	1	3	3	3	4	3	4	5	3	4	3	4	3	3	1	3	1	1	1	20
Los datos que se verifican después de realizadas las copias de seguridad se catalogan como:	3	1	3	3	3	1	3	1	3	3	1	3	1	3	3	1	3	1	1	3	20
El servicio prestado por el operador alterno en caso de que el principal falle lo podemos	1	1	3	3	3	4	3	4	3	2	4	4	1	3	3	1	3	1	1	3	20
En qué estado se encuentra el servidor alterno.	3	4	3	3	3	4	4	4	3	3	3	4	4	3	3	3	3	1	1	1	20
El Sistema de control para el ingreso a esta área se define como.	1	1	1	1	1	1	3	1	2	4	1	2	1	3	1	1	3	1	1	1	20
Como se define las pistas dejadas al ingresar a esta área	1	1	1	1	1	1	3	1	1	3	1	1	1	3	1	1	3	1	1	1	20
Como se definen los controles que se ejerce a los usuarios del área de TI para ingresar a los servidores.	1	1	1	1	1	1	3	1	1	1	1	1	3	3	1	1	3	1	1	1	20
3. Aplicación de Herramientas para la proteccion de datos y la Seguridad de la Informacion																					
El antivirus instalado en los equipos de cómputo de la empresa se puede definir como	1	1	2	1	1	4	4	4	4	4	5	4	4	4	1	1	1	4	1	1	20
El nivel de protección brinda el antivirus instalado en los equipos de computo	1	1	2	1	1	4	4	1	4	4	5	1	4	4	1	1	1	1	1	1	20
Como se define la restricción a paginas no permitidas en la empresa Market Mix	1	1	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	20
Los equipos de cómputo tienen licenciamiento vigente	4	4	4	4	5	4	4	5	5	4	5	4	4	1	4	1	1	1	1	1	20
Como se define el password para el ingreso al sistema	4	4	4	4	4	1	4	4	4	4	4	1	4	4	1	1	4	1	1	4	20
El nivel de seguridad cumple con los parámetros establecidos para el ingreso al sistema.	4	4	4	4	4	4	4	4	4	4	4	4	4	4	1	1	4	1	1	4	20

Anexo D. Cuestionario Área de TI

AREA:				
FUNCION A EVALUAR :				
AUDITADO :				FECHA :
CARGO :				HORA
OBJETIVOS:				
	S	N	N/A	Observaciones
Para la creación de usuarios hay una sola persona encargada para realizar esta actividad				
Hay registros de los usuarios creados				
Los usuarios que se encuentran en periodo de vacaciones o que ya no laboran en la empresa son bloqueados				
Debe solicitar permisos especiales para crear usuarios				
Las claves creadas tienen caducidad				
AUTENTICACION	S	N	N/A	
El password es genérico para todos los usuarios creados				
Está definido el tamaño y definición del password				
El ingreso de clave continua errada bloquea al usuario				
Los usuarios pueden ingresar a través de cualquier equipo				
Se puede ingresar a través de otro equipo de cómputo si el usuario ya está en uso				
AUTORIZACION	S	N	N/A	
Los usuarios creados tienen permiso para realizar cualquier clase de consulta, modificación o alteración de la base de datos				
Están definidos los permisos para cada usuario				

Hay autorización para el cambio de usuarios o password				
Está permitido a páginas que no son de orden institucional				
Se puede hacer uso de celular o cualquier medio de almacenamiento durante la jornada laboral				
PROFILES	S	N	N/A	
El administrador puede realizar cambios en la BD				
La sesión de los usuarios permanece activa durante tiempos prolongados cuando no hay uso del sistema				
Hay controles para el acceso a los backup por parte del DBA				
Los usuarios pueden extraer información a través de dispositivos externos				
Los usuarios pueden destapar o abrir los equipos de cómputo asignados				
QUOTAS	S	N	N/A	
Los equipos tienen la capacidad de memoria suficiente para la ejecución de programas y aplicaciones necesarias para ejecutarse correctamente				
Todos los procesos de la compañía se encuentran documentados				
Hay límite de conexión de usuarios a la base de datos				
PISTAS DE AUDITORIA	S	N	N/A	
El sistema cuanta con triggers				
Los proxys están definidos				
Se actualizan bitácoras para el registro o actualización de la información				
INTEGRIDAD				